Journal of Posthumanism
2025
Volume: 5, No: 3, pp. 475–509
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i3.759

The Impact of Cyber Risks as a Mediating Variable on the Relationship Between Spending on Cyber Security and Performance in Saudi Islamic Banks with A Field Study

Abdelaal Mostafa Aboelfadl[1], Faisal Abdullah Otaibi[2]

Abstract

The aim of the research is to identify the impact of spending on cybersecurity on cyber risks, and to find the mediating effect of cyber risks in the relationship between spending on cybersecurity and performance in Islamic banks. The focus was on both the inductive and deductive approaches in answering the research questions. The researcher used a survey form to collect data from the field study community represented by branch managers and deputy managers, department managers and bankers working in Saudi Islamic banks. A random sample of (260) individuals was identified from the study community, and (250) valid questionnaires were collected at a rate of (96%) of the total questionnaires. The results of the field study showed that the independent variables represented by (spending on prevention or detection of cybercrimes) and (spending on developing cybersecurity) had a positive impact on reducing cyber risks in Islamic banks. Reducing cyber risks also had a positive impact on financial and non-financial performance in Islamic banks. In terms of the relative importance of the degree of impact of spending on cybersecurity on cyber risks in Saudi Islamic banks, it came in first place. The impact of spending on prevention and detection of cybercrimes in reducing cyber risks was 4.76, followed by the impact of spending on developing cyber security in reducing cyber risks with an average of 4.70. In terms of the relative importance of the degree of impact of cyber risks on financial and non-financial performance in Saudi Islamic banks, the impact of cyber risks on financial performance was ranked first with an average of 4.95, followed by the impact of cyber risks on non-financial performance with an average of 4.78. The Kruskal-Wallis Test was conducted and showed no difference between the opinions of the research sample categories.

Keywords: *Cost of Cyber Security, Return on Cyber Security Investment, Cyber- Attacks, Cyber Security, Cyber Risks, Financial and Non-Financial Performance, Islamic Banks.*

Introduction

The provision of electronic banking services, or e-banking, along with electronic hardware facilities like automated teller machines (ATMs), electronic kiosks, personal digital assistants (PDAs), electronic wallets, etc., makes banking more convenient for customers and contributes significantly to the financial growth of banks (Soylemez & Ahmed, 2019; Nazaritehrani & Mashali, 2020). The primary obstacle to the financial growth of e banking is cybersecurity penetration, and banks have employed Financial institutions spend hundreds of millions of dollars a year on cybersecurity; therefore commercial cybersecurity is utilized to fight cybercrime (Khalil, Usman & Manzoor, 2020). (Columbus, 2020).

[1] Professor of Accounting, Shaqra University, Email: aabuelfadl@su.edu.sa.
[2] Assistant Professor of Accounting, Shaqra University

One of the contemporary methods for safeguarding data connected to Internet networks and information technology is cybersecurity. Information is shielded by cybersecurity from theft and illegal access to corporate organization systems. In this area, cybersecurity policy is regarded as one of the most innovative and modern policies since it safeguards in the context of information and communications technology, this policy satisfies the needs for information availability, trustworthiness, and secrecy. Additionally, this policy improves the output quality of information systems. Banks are required by central banks to have a cybersecurity policy, with the installation of anti-hacking tools being the most crucial component (Arab Monetary Fund, 2019; Al-Baghdadi, 2021).

Research Problem

The average cost of a single cyberattack on the financial sector reached $5.72 million in 2021, according to data from International Business, and the number of cyberattacks on financial institutions is increasing fourfold annually, per a 2020 Carnegie Endowment for International Peace study. IBM and "Ponemon"Foundation, demonstrating that data security has grown to be a significant concern for the banking industry. But the majority of financial institutions haven't made any efforts to improve their cybersecurity capabilities. Even while interest in cyber dangers has grown recently, many nations still haven't taken the required precautions to guard against these attacks.

Based on information released from an IMF survey of 51 countries in 2023, the majority of developing country financial officials have not resumed issuing cybersecurity regulations or taken action to enforce those regulations, and 56% of central banks or supervisory authorities at the level of The global financial sector lacks a national cyber strategy, 42% of countries lack a system specifically designed to manage cybersecurity risks, 68% lack a specialized risk unit, 64% have not tested their cybersecurity or offered recommendations to improve it, 54% lack a system specifically designed to report cyber incidents, and 48% lack cybercrime regulations. %6130353 at https://www.youm7.com/story/2023/3/28.

To stop cyberattacks, banks invest a lot of money in cybersecurity. The two components of cybersecurity costs are cybersecurity development costs (DC) and prevention and detection costs (PDC). Studies have shown that a small number of studies have been conducted on the cost/expenditure of cybersecurity and the financial performance of Islamic banks (Desta, 2018). Researchers have reported that very few studies measure the correlation between cybersecurity cost and performance for banks (Njoroge, 2017; Njoroge & Njeru, 2017; Odhiambo & Ngaba, 2019). Furthermore, there isn't any independent research in Egypt. The relationship between cybersecurity risk, spending, and performance in Islamic banks is measured by Researcher Science.

The fast digital transformation of banking operations necessitates a rise in cybersecurity spending, which may have a negative or positive impact on bank performance. Accordingly, researchers must investigate whether this spending growth is due to strategic necessity or not. This study examines the relationship between decreasing cybersecurity risks and raising cybersecurity spending. In addition, how can performance in Islamic banks be enhanced by lowering cybersecurity risks as an intermediary variable? the following primary question can be used to define the study problem in light of AIG (2016), BIS (2016), Fed (2017), and EU (2018): **What effect**

does cybersecurity spending have on Islamic banks' performance?

To answer the main research question, the following questions can be answered:

What is the impact of cybersecurity spending on cyber risks and hence on performance in Islamic banks?

In order to answer this question, it is necessary to answer the following two sub-questions:

- What is the impact of the costs of preventing and preventing cybercrimes on cyber risks in Islamic banks?

- What is the impact of cybersecurity development costs on cyber risks in Islamic banks?

What is the impact of cyber risks on performance in Islamic banks?

In order to answer this question, it is necessary to answer the following two sub-questions:

- What is the impact of cyber risks on the financial performance of Islamic banks?

- What is the impact of cyber risks on non-financial performance in Islamic banks?

Research Objective

The goal of the research is to identify the impact of cybersecurity spending on cyber risks, and to find the mediating effect of cyber risks in the relationship with cyber security costs and on performance in Islamic banks. This is achieved through the following objectives:

1. Know the impact of cybersecurity spending on cyber risks in Islamic banks.

To achieve this goal, the following two sub-goals must be achieved:

- Knowing the impact of the costs of preventing and preventing cybercrimes on cyber risks in Islamic banks.

- Knowing the impact of cybersecurity development costs on cyber risks in Islamic banks.

2. Knowing the impact of cyber risks on performance in Islamic banks.

To achieve this goal, the following two sub-goals must be achieved:

- Knowing the impact of cyber risks on financial performance in Islamic banks.

- Knowing the impact of cyber risks on non-financial performance in Islamic banks

The Importance of Research

The study contributes to the body of literature on the cost and expenditure of cybersecurity, which will be helpful to researchers conducting similar studies because it is the first to measure the impact of cybersecurity spending on cyber risks and performance. The research is significant for scholars because it offers up-to-date, comprehensive knowledge of the impact of cybersecurity spending on cyber risks and performance in Islamic banks while using cyber risk as an intermediate variable. This

research is crucial for Islamic banks since it helps to clarify how cybersecurity investment affects cyber risks and performance, and how crucial this information is for decision-making regarding.

Research Methodology

In order to address the study problems, both the deductive and the inductive approaches were prioritized. In order to create the theoretical framework and develop research hypotheses that must be tested in order to achieve the research objectives, the researcher uses the deductive approach, which is based on observation, scientific deduction, and extrapolation of reality through previous studies available in Arab and foreign research on a subject in scientific periodicals and websites related to the subject of the research. The inductive approach is used during the field study in order to test the research hypotheses on a sample of Islamic banks operating in Egypt and verify the validity or incorrectness of the research hypotheses.

Research Plan

To answer the research questions and achieve its objectives, the researcher organized the research as follows:

1. General research framework.

2. Saudi banking sector.

3. Previous studies.

4. The theoretical framework of cybersecurity and cyber risks.

5. The impact of cybersecurity spending on cyber risks in banks.

6. The impact of cyber risks as an intervening variable on the relationship between cybersecurity spending and performance in Islamic banks.

7. Field study.

8. Research results, recommendations and proposals for future research.

Saudi Banking Sector

There are currently (30) banks licensed by the Saudi Central Bank in the Kingdom of Saudi Arabia (https://n9.cl/lzbok) Of which (11) are local banks and (19) are branches of foreign banks. The licensed Saudi local banks are: https://n9.cl/lzbok

1. National Commercial Bank
2. SABB Bank
3. Saudi Investment Bank
4. Alinma Bank
5. Saudi Fransi Bank
6. Riyadh Bank
7. Al Rajhi Bank
8. Arab National Bank
9. Al Bilad Bank
10. Al Jazira Bank
11. Gulf International Bank

Four of which are purely Islamic banks: (https://n9.cl/v8y3z , https://n9.cl/zws1qf , Al Saleh, Fatima Nabil, Al Barrak, and Muhammad, 2022)

1. Al Rajhi Bank
2. Al Bilad Bank
2. Al Jazira Bank
4. Alinma Bank

These four banks represent a sample Research in the field study.

The difference between Islamic banks and Islamic banks

Many countries in the world have a dual banking system where Islamic banks work side by side with traditional banks. To know the essential differences between the two banks, a comparison is made between their financial operations. The following are the most important of these differences: https://n9.cl/wilfp, Al-Dharafi, Ahmed, 2018; Shehata, Hussein, 2006).

First: Doctrinal and moral differences

The Islamic faith is the intellectual framework of the Islamic bank. It does not deal with usury (interest), neither taking nor giving. It also refuses to finance forbidden projects, or those that would harm the Islamic community. It embodies the principles of Islamic ethics in its relations with its clients, such as honesty, sincerity, loyalty, trustworthiness, and contentment. It also does not exaggerate in calculating its commissions and expenses in return for the services it provides to clients. In addition, the Islamic bank, in the event of the insolvency of a trustworthy debtor who has no prior convictions, is committed to the words of God Almighty: (But if he is in hardship, then let there be postponement until it is easy for him) [Al-Baqarah: 280]. Traditional banks are based on purely secular materialistic foundations, so most of their transactions contradict the principles of Islamic belief. They deal with usury (interest), taking and giving, they eat it and are eaten by it, and many of their transactions involve uncertainty, gambling and ignorance. They also do not hesitate to finance forbidden projects, such as entertainment venues, beer factories, tobacco companies, etc. They also exaggerate in calculating their commissions and expenses in exchange for the services they provide to customers. It is not in their custom to wait for a time of ease, as they are arbitrary in collecting their loans, and do not give any additional grace period for payment except under unfair conditions for the debtor. Other than that, they rush to sue those who are late in paying, even if that leads to declaring them bankrupt and seizing their money and property in exchange for the debts they owe and their interest.

Second: Difference in purpose

Islamic banks aim to achieve fair distribution, contribute to building an Islamic society of solidarity, and achieve social and economic development. Then comes profit, which is considered an incentive for them to continue their activities. Therefore, Islamic banks are reviving the obligation of zakat and organizing its function because zakat is an Islamic obligation, and one of the Pillars of Islam. Islamic banks also provide good loans to the needy, and finance and support social projects, such as mosques, educational institutions, and charitable and cooperative societies. As for traditional banks, they mainly aim to achieve the maximum possible profit regardless of Islamic values and ideals, therefore they do not grant any good loans, and the loans they provide are not without interest, with arbitrariness in collecting the value of these loans and their interest on the due date, and in the event that the borrower is late in paying, the bank confiscates the guarantees it has, or sells them at a public auction at less than

their real price.

Third: Difference in the policies of investing money

The Islamic bank invests the money available to it by applying several Islamic investment policies, the most important of which are the policy of speculation, the policy of participation, the policy of profit, the policy of leasing, the policy of istisna', and others. All of these investment policies combine the capital element with the labor element, and the primary role in them is for the labor element. They are based on the just Islamic principle of "profit and loss," which contributes to achieving social and economic development by mobilizing capital and pushing it to flow into various productive projects. As for traditional banks, their most important policy in investing their money is the policy of lending with interest. This activity represents approximately 75% of the activities of these banks, despite the fact that there are terrible economic and social harms to interest, and these banks do not hesitate to finance activities that lead to the monopoly of goods, nor to limit their financing to a group of the very wealthy. This means that traditional banks are likely to harm society, rather than benefit it, and the main reason for this is that they are usurious banks, and usury never brings any good, but rather it is a source of evils and sins in every age.

Fourth: Difference in the scope of the relationship with the client

The Islamic bank takes a positive stance towards its clients, it searches for them, goes to them, shares with them the available investment opportunities, and is linked with them in a relationship that is dominated by the nature of participation based on the principle of bearing risk and sharing in the results, profit or loss, while the relationship that connects traditional banks with their clients is a relationship of debt and mutual material interest, and therefore they do not take any positive stance with this or that client unless there is a direct material interest for them in the first place.

Fifth: Difference in areas of activity

Islamic banks go beyond the circle of specialization that distinguishes traditional banks, meaning that the Islamic bank combines social, financial, economic, and banking activities, and therefore one of the basic features of the Islamic bank is that it is a bank with multiple functions and activities, and practices long-term financing, medium-term financing, and short-term financing, meaning that it plays the role of Islamic banks, investment banks, and development banks. Therefore, the Islamic bank is more active and contributes more to serving the community than traditional banks of all kinds. As for traditional banks, they are specialized banks, including Islamic banks, industrial banks, agricultural banks, and real estate banks. That is, each traditional bank operates in a specific field that it does not deviate from. However, it has not achieved any noteworthy success except for the exorbitant profits, most of which come from debt trading, i.e. usurious interest. However, it is going from setback to setback, due to the bankruptcy epidemic that is constantly sweeping it, in accordance with the Almighty's saying: (Allah destroys interest and gives increase for charities) [Al-Baqarah: 276].

It is clear from the above that Islamic banks differ from Islamic banks in several aspects, the most important of which is not dealing with usury (interest) and providing banking services that are compatible with Islamic law, and this is what distinguishes Islamic banks from Islamic banks.

1. Previous studies

Previous studies were divided into two types of studies: studies that dealt with cybersecurity risks and studies that dealt with the impact of cybersecurity on bank performance, and they were addressed as follows:

Previous Studies That Addressed Cybersecurity Risks

The study of Abu Musa (2004) is one of the pioneering studies in this field in the Arab region. It focused on identifying the main risks that threaten the security of electronic accounting information systems in Saudi Arabia. The most important risks were represented in entering incorrect data, destroying the data and outputs of the accounting system, sharing the same passwords by more than one employee, entering viruses, entering the system by unauthorized persons, and transferring the outputs to persons who are not permitted to view them. The study concluded that many companies suffer significant financial losses due to the hacking of their accounting information systems by internal and external parties. The study by Al-Rashidi and Al-Sayed (2019) focused on the impact of disclosing cybersecurity risks in financial reports on stock prices and trading volumes of Saudi IT companies and compared that with American companies. The study concluded that Saudi companies have weak disclosure of cybersecurity risks, which negatively affects stock prices and trading volume and thus financial performance. It also showed significant differences in the disclosure of cybersecurity risks between Saudi and American companies. It also showed positive effects of disclosing cybersecurity risk management on stock prices and the company's market value. The study by Ali and Ali (2022) aimed to study and test the impact of disclosing the cybersecurity risk management report on the decision to invest in shares of companies listed on the Saudi Stock Exchange, as well as testing the impact of some demographic characteristics (level of experience and academic qualification of the investor) as moderating variables on the relationship under study. The study concluded that there is a positive and significant impact of the cybersecurity risk management report. Cybersecurity on the decision to invest in stocks, as well as the moral impact of the investor's experience and level of academic qualification on the relationship between the disclosure of the cybersecurity risk management report and the decision to invest in stocks. The study by Mahrous and Saleh (2022) attempted to develop the performance of internal auditing in Saudi business organizations to confront cybersecurity risks, by using the Agile Approach as one of the modern development approaches, in addition to presenting a set of proposals that clarify the method and stages of applying agile internal auditing to confront cybersecurity risks. The study concluded that there were no significant differences between the opinions of the surveyed categories regarding the continuous increase in cybersecurity risks and their effects at the level of business organizations and at the national level, and there were no significant differences between the opinions of the surveyed categories regarding the shortcomings of traditional internal auditing in confronting cybersecurity risks. The study by Yaqoub and others (2022) sought to propose an index for disclosing cybersecurity risks within the information disclosed in the annual reports issued by economic units. The study concluded that there was an index for accounting disclosure of cybersecurity risks according to International requirements issued by professional bodies, legislation, foreign and Arab guides, and what was presented by (AICPA), the SEC guide, and the financial regulatory guidelines of the Toronto Stock Exchange

(TSX). The study of Amirhom (2022) aimed to test the impact of internal audit quality in reducing cybersecurity risks and its repercussions on rationalizing investor decisions. The results indicate that there are no significant differences between the opinions of internal audit officers, information technology officers, risk management officers, and investors through securities brokerage and trading companies, as the level of significance was greater than 0.05, and thus the four groups agreed on the existence of a relationship between reducing cybersecurity risks and rationalizing investor decisions. The study of Al-Rukban (2023) aimed to identify the reality of achieving cybersecurity for administrative information systems at Imam Muhammad bin Saud Islamic University, and to reveal the obstacles that limit its achievement. The descriptive survey approach was applied, and the study reached several results, including: the study individuals agreed to a high degree and with a general arithmetic average (4.14) on the reality of achieving cybersecurity For administrative information systems, with a general arithmetic mean (2.63) on the obstacles that limit the achievement of cybersecurity for administrative information systems, and also with a general arithmetic mean (3.81) on the proposals that contribute to achieving cybersecurity for administrative information systems.

Previous Studies That Addressed the Impact of Cybersecurity on Bank Performance

Njogu's study (2014) sought to measure the impact of electronic information systems on the profitability of Kenyan banks. The study concluded that there is a strong positive relationship between the speed of response to emerging variables in the banking environment and profitability indicators represented by the rate of return on assets and the rate of return on equity, and that there is a significant relationship between the ability of the information system to provide security and integrity of operations and the profitability of banks. As for the study of Arshid (2017), it aimed to identify the impact of investment in information technology (investment in hardware, investment in SW software and the number of ATMs) on the performance of Saudi banks, according to performance measures, which include return on assets and return on equity. It was concluded that there is a positive impact of investment in technology. Information (investment in hardware, investment in software and the number of ATMs) on improving services and increasing financial performance. Hassan's study (2021) addressed the relationship between investment in information technology and the financial performance of banks in different environments. This relationship was discussed by reviewing the most important foreign and Arab studies related to the topic, and identifying the impact of information and communications technology on the profits and risks of the banking industry in the European Union. The study concluded that there is a significant and positive role for investment in information technology in improving performance in banks operating in Europe. Bokhari & Manzoor's study (2022) focused on the impact of applying the ISO27001 standard (Requirements for an Effective Information Security Management System) on financial performance and improving banking reputation. The study concluded that low awareness among employees is the main obstacle to implementing effective information security risk management, as most managers prefer remedial rather than preventive methods, which increases the cost of damages. It also provided evidence of improved financial performance of banks using the return on assets rate and the return on equity rate. It was found that banks that implemented strong information security systems enjoyed strong financial performance and improved banking reputation. The study by Rashwan and Qasim (2022) addressed the impact of cybersecurity risk management on supporting and enhancing financial stability and inclusion in Palestinian banks,

as banks realize the danger of cyber breaches on stability. The study concluded that there is a significant impact of cybersecurity risk management on supporting and enhancing financial stability and inclusion in Palestinian banks. The study by Gatzert & Schubert (2022) explained the relationship between cyber risk management in American banks and insurance companies and awareness and its impact on financial performance, through the disclosure of cyber risk management information in the annual reports of large and medium-sized companies, and concluded that there is a significant positive relationship between cyber risk management and company value measured by Tobin Q, which positively affects financial performance.

Results of Previous Studies:

Through reviewing previous studies, the following was concluded:

- The topic of cybersecurity and cybersecurity risks has received a large amount of studies and research in many fields.

- Some studies relied on theoretical analysis of previous studies, while others relied on the use of statistical analysis of a number of actual data to reach conclusions regarding both cyber risks and cybersecurity.

- Many studies have addressed the impact of investment in information technology on performance in banks, and the components of investment in information technology were ATMs, mobile banking, online banking, debit and credit cards, etc.

- The scarcity of studies that addressed the relationship between cybersecurity, cyber risks, and performance in Islamic banks.

- Previous studies, to the best of the researcher's knowledge, did not address the impact of spending on cybersecurity on cyber risks and performance in Islamic banks.

What Distinguishes the Current Study from Previous Studies

From the review and analysis of previous studies, it becomes clear that they deal with cyber risks and the impact of cybercrimes on banks in general. Previous studies did not clarify the costs that banks must take into account when spending on cyber security to prevent or reduce cyber-attacks. Due to the lack of studies that deal with the impact of spending on cyber security on the performance of Islamic banks in light of the mediation of the cyber risk variable, the research seeks to fill this research gap and open the way for researchers to address this important topic from new dimensions.

Research Hypotheses

The research seeks to test the following hypotheses:

The first main hypothesis: Cybersecurity spending affects cyber risks in Islamic banks.

The first main hypothesis is divided into two sub-hypotheses:

1. The cost of preventing and detecting cybercrimes affects cyber risks in Islamic banks.

2. The cost of developing cybersecurity affects cyber risks in Islamic banks.

The second main hypothesis: Cyber risks affect financial and non-financial performance in Islamic banks.

The second main hypothesis is divided into two sub-hypotheses:

1. Cyber risks affect financial performance in Islamic banks.

2. Cyber risks affect non-financial performance in Islamic banks.

Theoretical framework of cyber security and cyber risks:

The theoretical framework for both cybersecurity and cyber risk will be addressed as follows:

Cybersecurity:

In this part, the concept, characteristics, axes, types and benefits of cybersecurity will be discussed as follows:

The Concept of Cybersecurity

Cybersecurity is concerned with designing and applying the necessary technologies, processes, controls, and practices to protect systems, networks, programs, devices, and data from exposure to attacks, electronic threats, and viruses, and filling the gaps of direct or indirect weaknesses. This is done through a set of procedures, including conducting a deliberate experimental attack to discover the gaps and work to fix them, and designing A set of response procedures and mitigation of the effects resulting from exposure to danger, damage, or unauthorized access , where the hacker seeks to manipulate the victim's digital system and control it illegally by using advanced devices or exploiting system vulnerabilities, or the user's low technological awareness (on , and in favor of), 2022).

The concept of cyber security for accounting systems expresses the degree of protection and security for managing accounting operations by providing appropriate technologies and software to ensure the prevention of internal and external cyber penetration of data, information, systems, hardware, software and accounting processes. Protection is achieved by using the cyber shield as an effective firewall to detect... Gaps (Alqahtani, F.H. (2017) Cybersecurity is the practice of securing computer systems and networks against unauthorized access, by mitigating information risks and vulnerabilities, and thus this practice has become an essential part of maintaining the safety of companies and individual users. https://cutt.us/6H4AY.

The researcher believes that cybersecurity is related to securing computer systems and networks through information and communications technology from exposure to electronic attacks, threats, and viruses, and filling gaps in direct or indirect weaknesses.

Characteristics of Cybersecurity

There are many characteristics of cybersecurity, the most important of which are (Kagwang, 2022; Alqahtani, FH, 2017):

1. Trust and mistrust: Cybersecurity treats all programs, technologies, links, etc. as untrustworthy, and thus only allows reliable ones to pass and prevents malicious ones from passing.

2. Protection from internal threats resulting from low user awareness or ignorance of information security, by alerting employees to the danger to prevent hacking, as it has been shown that the most dangerous cyber threats arise due to low employee awareness, which harms the reputation of companies.

3. Protection from external threats by building a firewall that works around the clock as an electronic filter for programs and technologies to filter external digital risks, and address vulnerabilities that a third party may exploit to control and control.

4. Achieving a comprehensive vision of the strengths, weaknesses, and potential technological gaps that affect the financial performance and economic decisions of information users, working to solve them as quickly as possible, and submitting proposals to prevent their recurrence.

Cybersecurity Policy Axes

There are many axes of cybersecurity policy, the most important of which are: (Abbas, 2010https://2u.pw/tWkeENZ; https://2u.pw/qui5BA2).

1. Defining roles and responsibilities, including responsibility for decision - making within the company regarding cyber risk management, including emergencies and crises.

2. Information management includes data governance and classification, in addition to the security and management of information and the information and communications technology environment in the company , with the aim of protecting data during the process of preparation, transfer, isolation and destruction, and tightening the control process over all electronic and non- electronic information resources, in addition to achieving the necessary security and protection of information from access or use. Unauthorized disclosure of information resources in the organization.

3. Privacy of customer data: This policy aims to preserve information related to customers and not disclose it to third parties, as well as ensuring that the privacy of the information is not violated by other employees who have nothing to do with the information.

4. Cyber risk management, in addition to protection controls to reduce and control cyber risks, as well as continuity and disaster recovery plans.

5. Determine the mechanism for disclosing the provisions of the cybersecurity policy to concerned parties.

6. Determine the owner, the scope of application, the periodicity of review and update, the powers of review and distribution, the objectives and responsibilities, the work procedures related to them, the penalties in the event of non- compliance, and the mechanisms for examining compliance.

Types of Cybersecurity

There are several different types of cybersecurity, which are as follows https://2u.pw/c5zCUHL :

The first type: Network Security

Most electronic attacks occur through electronic networks, so there must be a solution to this problem, and one of the best solutions is to rely on cybersecurity, as it helps protect all computer networks from attacks.

The second type: Cloud Security

In the recent period, there has been reliance on artificial intelligence, whether by individuals or by companies, and the goal of this is to improve the quality of work, accomplish many tasks, and enhancethe work experience. It is known that the amount of data that is stored is difficult to retain. Therefore, there are many different companies working to provide the best services that help solve this problem in record time, and here are the best of those services (Google Cloud) (Microsoft Azure).

The third type: application security

This type is one of the types of cybersecurity, as it is known that web applications are connected tothe Internet, Therefore, it may be hacked and data stolen. Here, if you ask about the importance of cybersecurity, this type helps companies protect data from any attack such as (viruses - information encryption) and others.

The Type Four: Operational Security

If the data is exposed to hacking, this type helps to reach many alternative plans, so it is relied upon in largest companies and institutions.

2. The impact of cybersecurity spending on cyber risks in Islamic banks

Since cybersecurity risks lead to systemic risks, financial institutions find that their spending on hardware, software, high-quality systems maintenance, and workforce training is indispensable for developing a more resilient operational infrastructure , and therefore researchers see that banks incur more fixed overhead expenses that can affect net profits (Keswani & Kumar, 2015), and in this regard, (Eling & Lehmann, 2018) analyze that assessing the intangible losses of cybersecurity failures is complex since the erosion of customer confidence in banks' ability to protect their money and confidential information has been It can lead to serious repercussions, and also in the event of cyber- attacks, some losses may be incurred due to the possibility of filing lawsuits and compensation claims by affected customers or other external parties (Kopp et al., 2017), and this means that banks need to analyze Benefits, costs and losses before allocating a budget for spending in cyber technology (Toivanen, 2015), however in practice banks maintain budget allocations to acquire the necessary technology without net present value analysis (Gordon & Loeb, 2002b), and thus banks often spend more is optimally required and affects profits (Gordon & Loeb, 2002a), and this type of research leads to a puzzling question for bank managers when they decide whether a marginal increase in spending on cybersecurity can lead to greater proportional added value (CarlColwill, 2009; Trautman & Altenbaumer 2010) , and the impact of spending in cybersecurity on cyber risks in Islamic banks will be addressed as follows:

Spending in Cybersecurity

Banks and financial institutions are constantly increasing their technology expenditures to overcome increasing cyber threats that increase fixed operating costs (Euro money, 2017). The Deloitte report shows that banks' technology expenditures (as a proportion of total revenues) rise to 7.16%, the highest among all sectors of the global economy (Kark et al., 2017). It therefore indicates that the global financial industry is negatively affected by both direct losses resulting from cybersecurity breaches and additional cyber overhead costs , and in general the body of literature that has been developed bears a general consensus that institutions bear an additional financial burden resulting

from rampant cyber incidents that Occurring due to the rapid digitization of operations and delivery of financial services , the situation is even worse because estimating economic losses resulting from a cybersecurity breach is very complex due to the multidimensional impacts of a security breach on banks' operational risks, costs, and performance (Lewis & Baker, 2013; Peng et al., 2017; Lever & Kifayat, 2020), which means that cybersecurity risks lead to escalation of operational risks, which in turn leads to higher operational costs to negatively impact the financial results of banks and financial institutions. (Kopp et al., 2017; Fitch, 2017; Aldasoro et al. al., 2020 a; Aldasoro et al., 2020 b)

The computer is used in cybercrimes either as a means to commit a crime, as a recording system, oras a target for the crime (Padmaavathy, 2019 Computers may either store data as a storage device that helps carry out a crime that their owners may not possess, such as intellectual property theft. Njoroge(2017) stated that in order to protect the electronic banking system from cyber-attacks, spending must be spent on cyber security to reduce its risks. Your spending budget in cybersecurity consists of: Njoroge, 2017).

1. Costs of cybercrimes (PDC).
2. Cybersecurity development costs (DC).

The types of spending in cybersecurity represented by costs will be discussed Prevention(prevention) and detection on Crimes Cyber and cost development Security Cyber in the next part.

Types of Spending in Cybersecurity:

Cybersecurity spending consists of two types of costs: cybercrime prevention and detection costs and cybersecurity development costs, and they are addressed as follows (Khalil, 2020):

1. Costs of Prevention and Detection of Cybercrimes:

The costs of preventing and detecting cybercrimes are defined as "the monetary equivalent of any efforts to avoid cybercrimes" (Lewis & Baker, 2013), and include the cost of updating computers by implementing an anti-virus system, and the cost of maintaining prevention measures (Anderson et al, 2013). The cost of preventing and detecting cybercrimes includes:

- Insurance premiums

- The cost of IT security systems such as spam filters, firewalls, antivirus software and browser extensions to protect users.

- The cost of data security audit evaluations.

2. Cost of Developing Cybersecurity:

These are costs related to quality and cybersecurity maintenance and include (Khalil, 2020):

1. The cost of analyzing and evaluating data and information security systems: The focus is on the appropriate data security infrastructure and includes the following costs: https://2u.pw/X40G5U0

- Costs of examining security vulnerabilities.

Penetration testing costs.

- Red team testing costs.

2. The cost of developing data and information security systems.

3. The cost of training employees on data security.

The researcher believes that spending in cybersecurity contributes to reducing cybersecurity risks, which has a positive impact on the financial and non-financial performance of Islamic banks, and the decrease in investment in cybersecurity contributes to increasing cyberrisks, which in turn leads to an increase in losses paid for cyberrisks. Therefore, it is necessary to briefly expose the losses resulting from the occurrence of cyber risks, as described in the next section.

Losses Resulting from Cyber Risks

Cyber risks result in two types of losses that banks bear:

1. Losses in response to cybercrime:

This takes into account direct losses incurred by individuals and businesses (including costs of business continuity and disaster response and recovery), as well as the costs of paying compensation to victims of identity theft, regulatory fines from industry bodies, and indirect costs associated with legal or forensic matters, including the cost of responding to crimes. Cyber include (Anderson et al, 2013 Khalil, 2020):

- Payment of compensation.

- Regulatory fines.

- Legal costs.

2. Indirect losses:

These include (Khalil, 2020; Lewis & Baker, 2013)

- Damage to reputation

- Loss of customer confidence

- Decrease in citizens' use of electronic services as a result of decreased confidence in online transactions

- Efforts to clean computers infected for the robot network.

The Volume of Spending in Cybersecurity

There are many factors that should be taken into consideration when determining the amount of spending in cybersecurity, including https://2u.pw/5M3ZhTz:

1. The myth that all assets in the bank are protected in the same way

A strong cybersecurity strategy should provide differentiated protection for a bank's most important assets, using a tiered set of security measures. Business and cybersecurity leaders must work together to identify and protect the "crown jewels" of banks that generate the most value for the bank.

2. The Myth: The more we spend, the safer we become

Some banks spend a significant amount on cybersecurity and actually underperform the rest of the market when it comes to developing digital resilience, partly because they are not protecting the right assets with a comprehensive approach (protecting all assets rather than protecting the crown jewels).

3. The myth that external hackers are the only threat to a bank's assets

There are significant threats from within the bank itself, and people closest to data or other bank assets are often a weak link in a bank's cybersecurity program, especially when they share passwords or files across unprotected networks or behave in other ways that open a bank's networks to attack.

4. The Myth: The more advanced our technology is, the safer we are

It is true that cybersecurity groups often use powerful and sophisticated techniques to protect a bank's data and assets, but it is also true that many threats can be mitigated using less advanced methods. According to research, more than 70% of global cyberattacks come from financially motivated criminals using methods... Technically simple, like phishing emails https://2u.pw/5M3ZhTz.

How do we manage the amount of spending on cybersecurity in Islamic banks?

Technology professionals have a role to play in re-educating senior banking officers on best practices in cybersecurity spending, specifically explaining why a tiered approach to cybersecurity is more effective than blanket coverage. A budget cannot grow or shrink depending on whether the bank has recently been exposed to breaches in the banking system, so the following must be taken into account https://2u.pw/5M3ZhTz:

- Cybersecurity spending should be considered permanent capital spending.

- Allocation priorities should be determined on the basis of a review of the full range of ongoing initiatives.

- Business and technology professionals must work together to manage the trade-offs associated with cybersecurity.

The cybersecurity team can engage executives in discussions about the most critical data assets associated with each part of the business value chain, the systems within them, the controls in place, and the trade-offs associated with protecting higher-priority versus lower-priority assets.

On a broader level, technology professionals can help senior bank officials set standards for cybersecurity spending in banks and on cybersecurity initiatives that can be reviewed regularly, and to have a comprehensive planning and review process for cybersecurity spending in banks. https://2u.pw/5M3ZhTz

The Role of Cybersecurity Spending in Reducing Cyber Risks

The International Monetary Fund estimates annual losses at 97 billion, which represents about 9% of global banks' net profits in 2018 (Bouveret, 2018), so banks are constantly increasing their technology expenditures to overcome increasing cyber threats that increase operating costs (Euromoney, 2017), and a Deloitte report shows that banks' technology expenditures (as a share of total revenues) rise to 7.16%, the highest among all sectors of the global economy (Kark et al., 2017).

Banks need to spend sufficiently on cybersecurity to reduce cyber risks by building a flexible online technological infrastructure as recommended by international organizations. Spending is mostly in areas such as acquiring the most reliable hardware and software, data encryption systems, and firewalls. Cyber monitoring, risk detection systems and IT training. (Paul & Wang, 2019; Ni et al., 2019), in other words, increasing spending on cybersecurity contributes to reducing cybersecurity risks as an intermediary variable, and decreasing cybersecurity risks improves financial and non-financial performance in banks. (Kopp et al., 2017; Fitch, 2017; Aldasoro et al., 2020a).

3. Spending on cybersecurity and performance in the banks in light of the mediation of cyber risks:

The relationship between cybersecurity spending, cyber risks and performance in the banks will be addressed as follows:

The Impact of Cybersecurity Spending on Cyber Risks in the Banks

Banks must maintain a high level of cybersecurity and put in place preventive measures to confront potential cyberattacks, design and implement cyber defense programs and mechanisms to maintain the safety and security of data and people, and then stabilize banks by conducting a review of the cybersecurity system (Cheng et al, 2022). In order to reduce cyber risks, the researcher believes it is necessary for banks to achieve cyber security through spending on it, which entails two types of costs: the costs of preventing and detecting cyber-crimes and the costs of developing cyber security, as spending on cyber security results in reducing cyber security risks.

The Impact of Reducing Cyber Risks on Performance in the Banks

Reducing cyber risks reduces the losses resulting from the occurrence of cyber risks in the banks, which are as follows:

- Losses in response to cybercrimes: which include (payment of compensation, regulatory fines, legal costs (Anderson et al, 2013 Khalil, 2020).

- Indirect losses: which include (damage to reputation, loss of customer confidence, a decrease in citizens' use of electronic services as a result of a decrease in confidence in online transactions, efforts made to clean computers infected with malware of a botnet that sends spam (Khalil, 2020 Lewis & Baker, 2013).

There is no doubt that reducing losses in response to cybercrimes leads to improving the financial performance of Commercial banks, while reducing indirect losses leads to improving the non-financial performance of Commercial banks, and this in itself calls on banks to increase spending on cybersecurity in advanced ways to mitigate the possibilities of security risks occurring. Cyber, and then improve the performance of banks.

In order to link spending on cybersecurity and performance in the banks in light of cyber risk, the research variables will be presented in the next section.

Research Variables

The researcher aims to determine whether the independent variables (the cost of prevention and detection, the cost of developing cybersecurity) have an impact on

cybersecurity risks and financial and non-financial performance in the banks, taking cybersecurity risks as an intermediary variable between spending on cybersecurity and performance in the banks. It is shown in Figure (1) below:

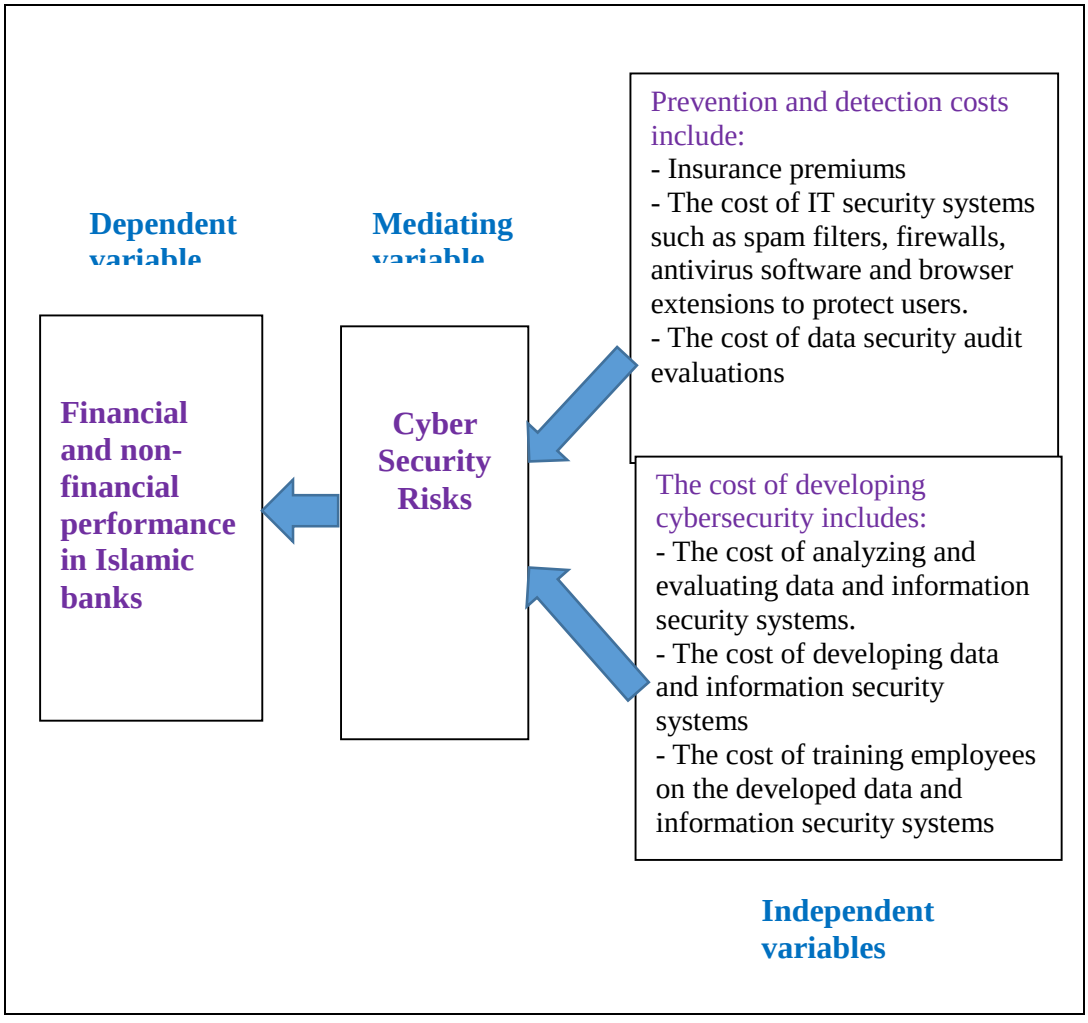

Figure No. (1) Spending on cybersecurity and performance in the banks, with cyber risks being an intermediary variable

Source: Prepared by the researchers

Figure No. (1) Shows that spending on cybersecurity consists of the costs of prevention and detection of cybercrimes, and the costs of developing cybersecurity. These costs represent the independent variables that have a direct impact on the dependent variable, which is cybersecurity risks. In addition, the risks Cybersecurity is an intermediary variable that affects financial and non-financial performance in the banks and spending on cybersecurity contributes to reducing cybersecurity risks, which in turn contributes to improving financial and non-financial performance in the banks, which is what the field study seeks to test its validity.

Summary of the Theoretical Study

The theoretical study concluded that increased spending in cybersecurity represented by hardware and software products designed to prevent cybercrime, anti-virus and phishing, malware infections, or unauthorized access to email accounts, as well as security measures in mitigating those risks (cost Purchasing and implementing cybersecurity technology), insurance costs and costs associated with compliance with information technology standards required for protection programs against hacking lead to reducing cyber risks. On the other hand, the study concluded that reducing cyber risks leads to improving performance in Commercial banks, whether financial performance or non-financial performance.

In the next section, the study variables are tested in the field on Saudi Islamic banks.

There is no doubt that the losses will be reduced Response For crimes Cyber technology leads to improving the financial performance of Islamic banks, while reducing losses not Directly leads to improving the non-financial performance of Islamic banks, And where that the average Growing continuously To change Technology Lead to more Activities Crimes e in sector Financial, and this is in Limit same He calls Banks to Increase spending in Security Cyber In ways Sophisticated To relieve from the odds happening Risks Security cyber, And from then to improve performance Banks .

In order to link spending in cybersecurity and performance in Islamic banks in light of the mediation of cyber risks, the following part will present the research variables, which are spending in cybersecurity, cyber risks, and performance in Islamic banks, which the research seeks to test to what extent they are valid or not.

Field Study

The field study aims to test the main research hypotheses, which are:

- The extent of the impact of cybersecurity spending on cyber risks in Islamic banks.

- The extent to which cyber risks affect the financial and non-financial performance of Islamic banks.

These main hypotheses were tested by testing a group of sub-hypotheses, each of which represents one of the sub-research variables, and finding field evidence that supports or rejects these hypotheses.

Statistical Methods

The following statistical methods were used in this research:

1. Descriptive statistical measurement based on statistical packages (SPSS) to describe the characteristics of the research sample and obtain arithmetic averages and standard deviations. The hypothetical arithmetic mean of (3) was relied upon as a standard for measuring and evaluating the score obtained by the respondents.

2. Kolmogorov-Smirnov test

3. Kruskal-Wallis Test to test the significance of differences between the means of the categories of respondents.

4. One-sample T-test to compare the calculated averages with the average tabular values applied

to test the research hypotheses.

Statistical Hypotheses for the Research:

The first main hypothesis: There is no statistically significant effect of cybersecurity spending on cyber risks in Islamic banks.

To test this hypothesis, the following two sub-hypotheses must be tested:

1. There is no statistically significant effect of the cost of preventing and detecting cybercrimes on cyber risks in Saudi Islamic banks.

2. There is no statistically significant effect of the cost of developing cybersecurity on cyber risks in Saudi Islamic banks.

The second main hypothesis: There is no statistically significant effect of cyber risks on performance in Saudi Islamic banks.

To test this hypothesis, the following two sub-hypotheses must be tested:

1. There is no statistically significant effect of cyber risks on financial performance in Saudi Islamic banks.

2. There is no statistically significant effect of cyber risks on non-financial performance in Saudi Islamic banks.

The third hypothesis: There are no fundamental differences between the opinions of the respondents about the impact of cybersecurity spending on cyber risks and financial and non-financial performance in Islamic banks.

Population and Sample of the Study

The field study community consists of branch managers, deputy managers, department managers, and bankers working in Saudi Islamic banks due to the availability and diversity of their experiences and awareness. A random sample of (260) individuals was identified from the study community, and (250) valid questionnaires were collected, representing (96%) of the total questionnaires, which is a good percentage for conducting statistical analysis. Table No. (1) Shows the distribution of survey forms received from the study sample according to the sample categories, which were as follows:

variable	Statement	the number	percentage
Qualification	Bachelor's	170	68%
	Master's	60	24%
	Ph.D	20	8%
	the total	250	%100
Job title	Branch Manager	35	14%
	Deputy Branch Manager	50	20%
	Head of the Department	60	24%
	banking	105	42%
	the total	250	%100
Years of Experience	From 5 – 10 years	115	46%
	15-10years	65	26%

	20-15years	40	16%
	Older than 20 years	30	12%
	Total	250	%100

Table No. (1) Distribution of survey forms received from the study sample

According to sample categories

Search Tool:

The data collection relied on a survey form that was prepared with simplicity, clarity and ease of understanding in mind. It was judged by a group of specialized judges until it came out in its final form. The five-point Likert scale was used, and the reliability of the questionnaire according to Cronbach's alpha was (0.85), which is an excellent percentage as it is higher than the acceptable percentage (60%), and this means that there is a high degree of reliability in the answers to the questions.

Testing the statistical hypotheses for the field study:

The statistical hypotheses of the field study were tested as follows:

The first main hypothesis: There is no statistically significant effect of spending on cybersecurity on cyber risks in Islamic banks.

To test this hypothesis, it is necessary to test the following two sub-hypotheses:

The first sub-hypothesis: There is no statistically significant effect of the cost of preventing and detecting cyber-crimes on cyber risks in Saudi Islamic banks.

Table No. (2) shows the results of the extent of the impact of the cost of preventing and detecting cyber-crimes on cyber risks in Saudi Islamic banks through the arithmetic mean, standard deviation, one-sample T-test, Kolmogorov-Smirnov test, and relative importance.

Statement	Arithmetic mean	Standard deviation	Relative importance	Calculated T value	Kolmogorov - Smirnov	Significant level
The costs of IT security systems such as spam filters, firewalls, and anti-virus software and browser extensions to protect users contribute to reducing cyber risks in Islamic banks.	4.95	0.11	0.97	23.45	0.96	0.00
Cybersecurity insurance costs contribute to reducing cyber	4.54	0.15	0.91	23.45	0.96	0.00

risks in Islamic banks.						
The costs associated with compliance with required IT standards contribute to reducing cyber risks in Islamic banks.	4.74	013	0.94	23.45	0.96	0.00
Maintenance costs and cybersecurity preventive measures contribute to reducing cyber risks in Islamic banks.	4.81	0.12	0.95	23.45	0.96	0.00
Average	4.76	0.13	0.94	23.45	0.96	0.00

Table No. (2) Results of the effect of the cost of preventing and detecting cybercrimes on cyber risks in Saudi Islamic banks

It was shown from Table No. (2) That the value of the arithmetic mean of the impact of the cost of preventing and detecting cybercrimes on cyber risks in Saudi Islamic banks was (4.76), compared to the hypothetical arithmetic mean of (3) as a standard for measuring and evaluating the score obtained, as well as the results of the sample T test. One and the results of the Kolmogorov- Smirnov test, which indicate that there are no fundamental differences between the sample items, the null hypothesis was rejected and the alternative hypothesis was accepted: There is a statistically significant effect of the cost of preventing and detecting cybercrimes on cyber risks in Saudi Islamic banks.

Second sub-hypothesis: There is no statistically significant effect of cybersecurity development costs on cyber risks in Saudi Islamic banks.

Table No. (3) Shows the results of the extent of the impact of cybersecurity development costs on cyber risks in Saudi Islamic banks, through the arithmetic mean, standard deviation, one-sample T-test, and relative importance

Statement	Arithmetic mean	Standard deviation	Relative importance	Calculated T value	Kolmogorov - Smirnov	Significant level
Vulnerability scanning costs contribute to reducing cyber risks in Islamic banks	4.85	0.09	0.96	23.45	0.96	0.00

Penetration testing costs contribute to reducing cyber risks in Islamic banks	4.66	0.13	0.91	23.45	0.96	0.00
The costs of data security audits contribute to reducing cyber risks in Islamic banks.	4.62	0.12	0.90	23.45	0.96	0.00
The costs of providing employees with the modern knowledge and skills necessary to prevent data breaches contribute to reducing cyber risks in Islamic banks	4.68	0.11	0.91	23.45	0.96	0.00
Average	4.70	0.11	0.92	23.45	0.96	0.00

Table No. (3) Results of the effect of cybersecurity development costs on cyber risks in Saudi Islamic banks.

It was shown from Table No. (3) that the value of the arithmetic mean for the extent of the results of the impact of cybersecurity development costs on cyber risks in Saudi Islamic banks amounted to (4.70), compared to the hypothetical arithmetic mean of (3) as a standard for measuring and evaluating the degree obtained, as well as the results of the T- test for the sample. One and the results of the Kolmogorov-Smirnov test, which indicate that there are no fundamental differences between the sample items, the null hypothesis was rejected and the alternative hypothesis was accepted: There is a statistically significant effect of the costs of developing cybersecurity on cyber risks in Saudi Islamic banks.

From the results of Tables No. (2) and No. (3), the first main hypothesis can be tested: There is no statistically significant effect of spending on cybersecurity on cyber risks in Islamic banks.

Statement	Arithmetic mean	Standard deviation	Relative importance	Calculated T value	Kolmogorov - Smirnov	Significant level

Average results of how the cost of preventing and detecting cybercrimes affects cyber risks In Saudi Islamic banks	4.76	0.13	0.96	23.45	0.96	0.00
Average results of the impact of cybersecurity development costs on cyber risks In Saudi Islamic banks.	4.70	0.11	0.92	23.45	0.96	0.00
Average	4.73	0.12	0.94	23.45	0.96	0.00

Table No. (4) Results of the effect of cybersecurity spending on cyber risks

In Saudi Islamic banks

It was shown from Table No. (4) that the value of the arithmetic mean of the extent to which spending in cybersecurity affects cyber risks in Islamic banks amounted to (4.73), compared to thehypothesized arithmetic mean of (3) as a standard for measuring and evaluating the degree obtained, as well as the results of the one-sample T- test and the results of Kolmogorov-Smirnov test, which indicates that there are no significant differences between the sample items. The null hypothesis was rejected and the alternative hypothesis was accepted: There is a statistically significant effect of spending in cybersecurity on cyber risks in Saudi Islamic banks.

The second main hypothesis: There is no statistically significant effect of cyber risks on performance in Saudi Islamic banks.

To test this hypothesis, it is necessary to test the following two sub-hypotheses:

The first sub-hypothesis: There is no statistically significant effect of cyber risks on financial performance in Saudi Islamic banks.

Table No. (5) shows the results of the extent of the impact of cyber risks on financial performance in Saudi Islamic banks through the arithmetic mean, standard deviation, T-test for one sample, and relative importance.

Statement	Arithmetic mean	Standard deviation	Relative importance	Calculated T value	Kolmogorov - Smirnov	Significant level
Reducing cybersecurity risks contributes to increasing the market value of the bank's	4.98	0.10	0.95	0.96	23.45	0.00

shares						
Reducing cybersecurity risks contributes to reducing the amount of compensation paid	4.96	0.15	0.94	0.96	23.45	0.00
Reducing cybersecurity risks contributes to reducing the value of regulatory fines	4.96	0.13	0.92	0.96	23.45	0.00
Reducing cybersecurity risks reduces legal costs	4.97	0.10	0.92	0.96	23.45	0.00
Reducing cybersecurity risks reduces disaster response costs.	4.93	0.10	0.91	0.96	23.45	0.00
Reducing cybersecurity risks contributes to reducing business continuity costs.	4.91	0.13	0.92	0.96	23.45	0.00
Reducing cybersecurity risks contributes to increasing the bank's profitability.	4.95	0.09	0.92	0.96	23.45	0.00
Reducing cybersecurity risks contributes to increasing the rate of return on investment in the bank.	4.93	0.08	0.95	0.96	23.45	0.00
Reducing cybersecurity risks contributes	4.97	0.07	0.96	0.96	23.45	0.00

to increasing the bank's rate of return on equity						
Average	4.95	0.10	0.93	0.96	23.45	0.00

Table No. (5) Results of the effect of cyber risks on financial performance

In Saudi Islamic banks.

Table No. (5) shows that the arithmetic mean value of the extent of the impact of cyber risks on financial performance reached (4.95) and compared to the hypothetical arithmetic mean of (3) as a criterion for measuring and evaluating the obtained degree, as well as the results of the T-test for a single sample and the results of the Kolmogorov-Smirnov test, which indicate the absence of fundamental differences between the sample items, the null hypothesis was rejected and the alternative hypothesis was accepted: There is a statistically significant effect of cyber risks on financial performance in Saudi Islamic banks.

Second sub-hypothesis: There is no statistically significant effect of cyber risks on non-financial performance in Saudi Islamic banks. To measure the extent of the impact of cyber risks on non-financial performance in Saudi Islamic banks, the general arithmetic mean, standard deviation, relative importance, and a single-sample T-test were calculated for the sample under study and application, and the results were as shown in Table No. (6).

Statement	Arithmetic mean	Standard deviation	Relative importance	Calculated T value	Kolmogorov - Smirnov	Significant level
Reducing cybersecurity risks contributes to enhancing customer satisfaction	4.90	0.12	0.91	0.96	23.45	0.00
Reducing cybersecurity risks contributes to enhancing employee satisfaction	4.72	0.14	0.89	0.96	23.45	0.00
Reducing cybersecurity risks contributes to improving the bank's reputation.	4.72	0.16	0.89	0.96	23.45	0.00
Reducing cybersecurity risks supports positive tracking from	4.82	0.09	0.90	0.96	23.45	0.00

the bank's financial experts						
Reducing cybersecurity risks contributes to attracting new customers	4.74	0.12	0.93	0.96	23.45	0.00
Reducing cybersecurity risks contributes to increasing citizens' use of electronic services.	4.81	0.09	0.91	0.96	23.45	0.00
Reducing cybersecurity risks reduces efforts to clean computers infected for the robot network.	4.75	0.11	0.94	0.96	23.45	0.00
Average	4.78	0.12	0.91	0.96	23.45	0.00

Table No. (6) Results of the extent of the effect of cyber risks on non-financial performance in Saudi Islamic banks

Table No. (6) shows that the value of the general arithmetic mean for the range of results of the extent of the impact of cyber risks on non-financial performance amounted to (4.78), compared to the hypothetical arithmetic mean of (3) as a criterion for measuring and evaluating the obtained score, as well as the results of the one-sample T-test and the results of the Kolmogorov test. - Smirnov, which indicates that there are no fundamental differences between the sample items. The null hypothesis was rejected and the alternative hypothesis was accepted: There is a statistically significant effect of cyber risks on non-financial performance in Saudi Islamic banks.

From the results of Tables No. (5) and No. (6), the second main hypothesis can be tested: There is no statistically significant effect of cyber risks on performance in Saudi Islamic banks, as the extent of the impact of spending on cyber security on cyber risks in Islamic banks is evident through the arithmetic mean, standard deviation, T-test for one sample, and the relative importance of the two tables.

Statement	Arithmetic mean	Standard deviation	Relative importance	Calculated T value	Kolmogorov - Smirnov	Significant level
middle Results of the impact of cyber risks on financial performance in	4.95	0.10	0.93	0.96	23.45	0.00

Saudi Islamic banks						
middle Results of the impact of cyber risks on non-financial performance in Saudi Islamic banks	4.78	0.12	091	0.96	23.45	0.00
the total	4.87	0.11	0.92	0.96	23.45	0.00

Table No. (7) Results of the extent to which cyber risks effect financial and non-financial performance in Saudi Islamic banks.

It was shown from Table No. (7) that the value of the arithmetic mean of the extent to which cyber risks affect financial and non-financial performance in Saudi Islamic banks reached (4.87), compared to the hypothetical arithmetic mean of (3) as a standard for measuring and evaluating the score obtained, as well as the results of the T- test for the sample. One and the results of the Kolmogorov-Smirnov test, which indicate that there are no fundamental differences between the sample items, the null hypothesis was rejected and the alternative hypothesis was accepted: There is a statistically significant effect of cyber risks on financial and non-financial performance in... Saudi Islamic banks.

The third hypothesis: There are no fundamental differences between the opinions of the respondents regarding the impact of spending on cybersecurity on cyber risks and financial and non-financial performance in Islamic banks.

To measure the absence of significant differences between the opinions of the respondents, the Kruskal -Wallis Test was conducted to test the significance of the differences between the means of the three categories of respondents, and the results of the test were as shown in Table No. (8).

Categories	the number	Average rank	Degrees of freedom	Ka^2	Significant level
Branch Manager	35	61.1	3	2.56	3.19
Deputy Branch Manager	50	56.3			
Head of the Department	60	58.7			
banker	105	64.7			
	250				

Table No. (8) Results of no differences among the respondents' opinions on the effect of cybersecurity spending on cyber risks and financial and non-financial performance in Islamic banks

Table No. (8) shows the results of the variance between the opinions of respondents in the fourcategories through the "Kruskal-Wallis Test" ,where the value of Ka^2 was (2.56), which is less than the level of significance of (3.19), and from this it is clear that there is no difference .Among the opinions of the research sample categories, the opinions of

the four categories of branch managers and deputy managers, department managers, and bankers working in banks were compatible, which supports the research results.

The extent of the impact of cybersecurity spending on cyber risks in Saudi Islamic banks can be ranked according to the degree of relative importance, as shown in Table No. (9).

Statement	Arithmetic mean	Relative importance	Ranking of relative importance
The impact of spending on prevention and detection of cybercrimes in reducing cyber risks in Islamic banks	4.76	0.96	1
The impact of spending on developing cybersecurity in reducing cyber risks in Islamic banks	4.70	0.92	2

Table No. (9) Ranking of the extent of the effect of cybersecurity spending on cyber risks in Saudi Islamic banks

Table No. (9) shows the relative importance of the degree of impact of cybersecurity spending on cyber risks in Saudi Islamic banks, as it came In first order The impact of spending on prevention and detection of cybercrimes in reducing cyber risks in Saudi Islamic banks has an average of (4.76), and in second place is the impact of spending in developing cybersecurity in reducing cyber risks in Saudi Islamic banks with an average of (4.70).

Also possible to rank the extent to which cyber risks affect financial and non-financial performance Saudi Islamic banks, according to the degree of relative importance, as shown in Table No. (10).

Statement	Arithmetic mean	Relative importance	Ranking of relative importance
Effect Cyber risks to financial performance in Saudi Islamic banks	4.95	0.93	1
Effect Cyber risks to financial performance in Saudi Islamic banks	4.78	0.91	2

Table No. (10) Ranking of the extent of the effect of cyber risks on financial and non-financial performance in Banks Commercial Egyptian.

Table No. (10) shows the relative importance of the degree of impact of cyber risks on financial and non-financial performance in Saudi Islamic banks, In the first place was the impact of cyber risks on the financial performance in Saudi Islamic banks with an average of (4.88), and in the second place was the impact of cyber risks on non-financial performance in Saudi Islamic banks with an average of (4.53).

Summary and Results of the Research and Suggestions for Future Research

Research Summary

Spending on cyber security and cyber risks and their impact on financial and non-financial performance in Saudi Islamic banks was addressed. Cyber security risks lead to increased operational risks, which in turn lead to higher operational costs. Increasing spending on cybersecurity contributes to reducing cybersecurity risks, and cybersecurity risks, as an intermediary variable, contribute to improving financial and non-financial performance in Islamic banks.

Consists of the cost of prevention and detection of cybercrimes and the cost of developing cybersecurity. Banks also bear losses resulting from increased cybersecurity risks, represented by losses in response to cybercrimes and indirect losses. There is no doubt that spending in cybersecurity It contributes to reducing cybersecurity risks, which will have a positive impact on the financial and non-financial performance of Islamic banks, and the decrease in spending on cybersecurity contributes to increasing cyber risks, which in turn leads to an increase in the losses paid for cyber risks.

The relationship between investment in cybersecurity, cyber risks, and performance in Islamic banks was analyzed, the factors that should be taken into consideration when determining the volume of spending in cybersecurity, how to manage the volume of spending in cybersecurity in banks, and the role of the return on security investment in making the investment decision in cybersecurity.

The results of the field study showed that all independent variables (spending on preventing and detecting cybercrimes and spending on developing cybersecurity) It had a positive impact in reducing cyber risks in Islamic banks. Reducing cyber risks also had a positive impact on the financial and non-financial performance of Islamic banks.

Search Results

The results of the research can be presented in the following points:

In terms of measuring the extent of the impact of cybersecurity spending on cyber risks and financial and non-financial performance in Saudi Islamic banks, the results of the field study were as follows:

There is a statistically significant effect of the cost of preventing and detecting cybercrimes on cyber risks in Saudi Islamic banks.

There is a statistically significant effect of cybersecurity development costs on cyber risks in Saudi Islamic banks.

There is a statistically significant effect of cybersecurity spending on cyber risks in Saudi Islamic banks.

There is a statistically significant impact of cyber risks on the financial performance of Saudi Islamic banks.

There is a statistically significant impact of cyber risks on non-financial performance in Saudi Islamic banks.

There is a statistically significant impact of cyber risks on the financial and non-

financial performance of Saudi Islamic banks.

In terms of the relative importance of the impact of cybersecurity spending on cyber risks in Saudi Islamic banks, the results were as follows:

In first order came The effect of spending on prevention and detection of cybercrimes in reducing cyber risks in Saudi Islamic banks with an average of (4.76) in second order came The effect of spending on developing cybersecurity in reducing cyber risks in Saudi Islamic banks has an average of (4.70).

In terms of the relative importance of the degree of impact of cyber risks on financial and non-financial performance in Saudi Islamic banks, the results were as follows:

The impact of cyber risks on the financial performance of Saudi Islamic banks came in first place, with an average of (4.95).

The impact of cyber risks on non-financial performance in Saudi Islamic banks came in second place, with an average of (4.78).

Cyber risks play an important role as an intermediary variable between spending in cybersecurity and performance in Islamic banks, as it leads to... Spending on cybersecurity reduces cyber risks, which in turn contributes to improving the financial and non-financial performance of Islamic banks.

The Kruskal-Wallis Test was conducted and it was found that there was no difference between the opinions of the categories of the research sample, and therefore the opinions of the four categories of branch managers and deputy managers, department managers and bankers working in the banks were compatible opinions, which supports the results of the research.

Proposals for Future Research

Based on the results of the research and through what was learned from previous studies, a group of future research can be proposed, for example, as follows:

1. Do more Studies on areas of spending in cybersecurity.
2. Conduct further studies on cyber risk areas in Islamic banks.
3. The impact of cybersecurity spending on the strategic performance of non-financial institutions.
4. Conduct an applied study to calculate the return on security investment in financial institutions and business companies.
5. The impact of companies' disclosure of the cybersecurity risk management report on the return on security investment.

References

Abu Musa, Ahmed slave Peace, (2004), Importance Risks Organized the information Accounting e, study Applied on Facilities Saudi Arabia, magazine commerce and Finance, College of Commerce, university Tanta, (2): 1-54.

Agboola, A. (2007). Information and communication technology (ICT) in banking operations in Nigeria– An evaluation of recent experiences. African Journal of Public Administration and Management, 18(1), 1-102.

Al-Baghdadi, Marwa Fathi Al Sayed, (2021), Economics Security Cyber in sector banker, magazine Research Legal and economic, college Rights, university Mansoura, (76):.1513-1466

AIG. (2016, December). Is Cyber Risk Systemic? New York: American International Group. Retrieved from https://www.aig.com/content/dam/aig/america- canada/us/documents/business/cyber/aigcyber-risk-systemic-final.pdf

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020a). Operational and cyber risks in the financial sector. BIS Working Paper No. 840. Basel, Switzerland: Bank for International Settlements.

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020b). The drivers of cyber risk. BIS Working Paper No. 865. Basel, Switzerland: Bank for International Settlements.

Ali, M. Hammoud Ahmed; And Ali, Saleh Ali, (2022), The impact of disclosing the cybersecurity risk management report on the decision to invest in shares of companies listed on the Egyptian Stock Exchange: An experimental study, Alexandria Journal of Accounting Research, Faculty of Commerce, Alexandria University, 6(3): 1-48.

Alqahtani, F. H. (2017). Developing an information security policy: A case study approach. Procedia Computer Science, 124, 691-697.

Al-Rashidi, Tariq Abdel-Azim Youssef, and Al-Sayed, Dalia Adel Abbas, ,(2019) The impact of disclosing cybersecurity risks in financial reports on stock prices and trading volumes: a comparative study in the information technology sector. Journal of Accounting and Auditing, (2): 439-487.

Al-Rukban, Al-Jawhara bint Othman bin Ali, (2023), investigation Security Cyber For systems the information Administrative in university Imam Mohammed son Saud Commercial : a study Evaluation magazine Arabic For studies Educational and social, (20) 159 - 209 retrieved from http://: search.mandumah.com/Record1353685

Altobishi, T., Erboz, G., & Podruzsik, S. (2018). E-Banking effects on customer satisfaction: The survey on clients in Jordan Banking Sector. International Journal of Marketing Studies, 10(2), 151-
161. https://doi.org/10.5539/ijms.v10n2p151

Amirhom, Jihan Adel, (2022), Effect Quality Review Interior in limit from Risks Security Cyber and its repercussions on Rationalization Decisions Investors: a study field, magazine Research Finance and Commerce, 23(3): 377-325 retrieved from http://search.mandumah.com/Record13

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M. & Savage, S. (2013). Measuring the cost of cybercrime. In The economics of information security and privacy (pp. 265-300).

Archie, Jackson, (2023), Does RoSI (on Security Investment) analysis help in decision making ?, Stay Aware | Stay Secure, A Cyber Security Newsletter, https://2u.pw/kMR8pQ4

Arshid, Muhammad (2017) Impact Investment in technology the information on performance Drains Saudi Arabia, the magazine Arabic Management, 37(1):.223-207

Ashford, W. (2019, July 31). Financial services top cyber-attack target. Computer Weekly. Retrieved from https://www.computerweekly.com

Badawy, H. (2021). The Impact of Assurance Quality and Level on Cybersecurity Risk Management Program on Non-Professional Egyptian Investors' Decisions: An Experimental Study. Alexandria Journal of Accounting Research.3(5):1-56.

Banqa, Alam El-Din, (2019), The Risks of Electronic (Cyber) Attacks and Their Economic Impacts: A Case Study of the Gulf Cooperation Council Countries, Development Studies Series, Arab Planning Institute in Kuwait, 63.

BIS. (2016, June). Bank for International Settlements. Retrieved from www.bis.org: https://www.bis.org/cpmi/publ/d146.pdf

Boin, A., & McConnell, A. (2007). Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis

Management and the Need for Resilience. Journal of Contingencies and Crisis Management, 15(1):50-59.

Bokhari, S.A., & Manzoor, S. (2022). Impact of information security management system on firm financial performance: perspective of corporate reputation and branding. American Journal of Industrial and Business Management, 12(5), 934-954.

Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. IMF Working Paper No. WP/18/143. International Monetary Fund.

Box Monetary Al-Araba, (2019), series the summary Policies around security outer space Cyber in sector Banker, (4).

Brechbuhl, H., Bruce, R., Dynes, S., & Johnson, M. E. (2010). Protecting Critical Information Infrastructure: Developing Cybersecurity Policy. Information Technology for Development, 16(1), 83-91.

CarlColwill. (2009). Human factors in information security: The insider threat – Who can you trust these days? Information Security Technical Report, 14(4), 186-196.

Cheng, X., Hsu, C., & Wang, T. D. (2022). Talk too much? The Impact of Cybersecurity Disclosures on Investment Decisions. Communications of the Association for Information Systems, 50 (1), 26

Columbus, L. (2020). Top 10 Cyber Security companies to watch in 2020 https://www.forbes.com/sites/louiscolumbus/2020/01/26/top-10-CyberSecurity-companies-to- watch-in2020/#3d820fd24fe6

Desta, N. D. (2016). Information safety, corporate image, and intention to use online services: Evidence from travel industry in Vietnam.

Desta, Y. (2018). Customers' e-banking adoption in Ethiopia, PhD Dissertation, Addis Ababa University, Ethiopia.

Donge, Z., Luo, F., & Liang, G. (2018). Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems. Journal of Modern Power Systems and Clean Energy, 1-10.

Eling, M., & Lehmann, M. (2018). The Impact of Digitalization on the Insurance Value Chain and the Insurability of Risks. The Geneva Papers on Risk and Insurance-Issues and Practice, 43(3), 359- 396.

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? European Journal of Operational Research, 272(3), 1109-1119.

Euromoney. (2017, August 1). Technology investments drive up banks' costs. Euromoney magazine. London.

EU. (2018, May). The Directive on security of network and information systems (NIS Directive).

Retrieved from https://ec.europa.eu/digital-single-market/en/network-and-information-security- nis-directive

Fed. (2017, September). Federal Reserve Policy on Payment System Risk. Washington, USA: Federal Reserve System. Electronic copy available at: https://ssrn.com/abstract=3689162

Fitch. (2017, April). Cybersecurity an Increasing Focus for Financial Institutions. Retrieved from https://www.fitchratings.com/site/pr/1022468

- Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. Journal of Risk and Insurance, 89(3), 725-763.

Germano, J. H. (2014). Cybersecurity Partnerships: A New Era of Public-Private Collaboration. New York: New York University School of Law.

Gladstone, R. (2016, March 15). Bangladesh Bank Chief Resigns After Cyber Theft of $81 Million. The New York Times.

Geyres, S., & Orozco, M. (2016). Think banking cybersecurity is just a technology issue? Think again.

accenture strategy. Retrieved from https://www.accenture.com/t20160419t004021 w /usen/_acnmedia/pdf-13/accenture- strategy-cybersecurity-in-banking.pdf
Gopalakrishnan, R., & Mogato, M. (2016, May 19). Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat. Reuters: Business News. Thomson Reuters
Gordon, L. A., & Loeb, M. P. (2002a). The economics of information security investment. ACM Transactions on Information and Systems Security, 5(4), 438-457.
Gordon, L. A., & Loeb, M. P. (2002b). Return on information security investments, myths vs realities. Strategic Finance, 84(5), 26-31.
Hassan, Mohammed Amen Robin, (2021), Effect Investment in technology the information on the performance Financial: a study Applied on Banks included in Market Palestine, magazine the university Commercial for studies Economic Management,109-83 :(1)30
Johnson, K. N. (2015). Managing Cyber Risk. Georgia Law Review, 50(2), 548-592.
Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. International Journal of Accounting & Information Management, 28(2), 275-301.
Kamiya, S., KangJun-Koo, Jungmin, K., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target companies. Journal of Financial Economics, In Press.
Kark, K., Shaikh, A., & Brown, C. (2017, November 28). Technology budgets: From value preservation to value creation. Deloitte Insight. London.
Khalil, K., Usman, A., & Manzoor, S. R. (2020). Effect of cyber security costs on performance of E- banking in Pakistan. Journal of Managerial Sciences, 14. 26-40
Kejwang, B. (2022). Effect of cybersecurity risk management practices on performance of insurance sector: A review of literature. International Journal of Research in Business and Social Science (2147-4478), 11(6), 334-340
Kesswani, N., & Kumar, S. (2015). Maintaining Cyber Security: Implications, Costs and Returns. Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research (pp. 161-164, New York: Association for Computer Machinery
Khalil, K. (2020). Effect of cyber security costs on performance of e-banking in Pakistan. Journal of Managerial Sciences, 14(4), 85-99.
Khalil, K., Usman, A., & Manzoor, S. R. (2020). Effect of cyber security costs on performance of E- banking in Pakistan. Journal of Managerial Sciences, 14. 26-40.
Khalid Khalil, Sheikh Raheel Manzoor, Muhammad Tahir, Nisar Khan, Khalid Jamal, (2021), MPACT OF CYBER SECURITY COST ON THE FINANCIAL PERFORMANCE OF E-BANKING: MEDIATING
INFLUENCE OF PRODUCT INNOVATION PERFORMANCE, Humanities & Social Sciences Reviews, 9(2)): pp 691-703 https://doi.org/10.18510/hssr.2021.9266
Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability, Working Paper. International Monetary Fund (WP/17/185).
Kox, H. L. (2013). Cybersecurity in the perspective of Internet traffic growth. Working paper. CPB Netherlands Bureau for Economic Policy Analysis. Retrieved from https://mpra.ub.unimuenchen.de/47994/
Lewis, J., & Baker, S. (2013). The Economic Impact of Cybercrime and Cyber Espionage. McAfee.
Lever, K. E., & Kifayat, K. (2020). Identifying and mitigating security risks for secure and robust NGI networks. Sustainable Cities and Society, 59, 102098.
Low, P. (2017). Insuring against cyber-attacks. Computer Fraud & Security (4), 18-20.
Macaulay, T. (2018). Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating

Risks, and Interdependencies (1st ed.). Boca Raton: Taylor and Francis Group.
Mahrous , Ramadan Arif Ramadan, And Saleh , Abu Al-Hamad Mustafa, (2022), Using the agile methodology in developing internal audit performance to confront cybersecurity risks, Journal of Financial and Business Research, 23(3):491:432
Moore, T., Clayton, R., & Anderson, R. (2010). The economics of online crime. The Journal of Economic Perspectives, 23(3), 3-20.
Nazaritehrani, A., & Mashali, B. (2020). Development of E-banking channels and market share in developing countries. Financial Innovation, 6(1), 12. https://doi.org/10.1186/s40854-020-0171-z
Ni, J., Lin, X., & Shen, Njoroge, E. W. (2017). Effect of cyber security related costs on development of product innovation performances and services: A case study of NIC bank of Kenya. PhD Dissertation. Kenyatta University of Agriculture and Technology.

.Njoroge, E., & Njeru, A. (2017). The impact of cybercrime response costs for the development of financial products: A case of NIC bank of Kenya. Journal of Managerial Sciences, 14(2), 33-51.
Njoroge, M. N., & Mugambi, F. (2018). Effect of electronic banking on financial performance in Kenyan Islamic banks: Case of equity bank in its Nairobi central business district branches, Kenya. International Academic Journal of Economics and Finance, 3(2), 197-215.
Njogu, N. J. (2014). "The Effect of Electronic Banking on Profitability of Islamic banks in Kenya". Master of Science in Finance, School of Business, University of Nairobi
OFR. (2017). Cybersecurity and Financial Stability: Risks and Resilience. Office of Financial Research.
Padmaavathy, P. A. (2019). Cyber Crimes: A Threat to The Banking Industry. International Journal of Management Research and Reviews, 9(4), 1-9.
Page, J., Kaur, M., & Waters, E. (2017). Directors' liability survey: Cyber-attacks and data loss — a growing concern. Journal of Data Protection & Privacy, 1(2), 173-182.
Paul, J. A., & Wang, X. (2019). Socially optimal IT investment for cybersecurity. Decision Support Systems, 122, 113069.
Peng, C., Xu, M., Xu, S., & Hu, T. (2017). Modeling and predicting extreme cyber-attack rates via marked point processes. Journal of Applied Statistics, 44(14), 2534-2563
Qasim, Samer Ahmed, and Ibrahim, Ayham Youssef, (2022), The role of information technology in improving the efficiency of banking innovations: A field study on public banks in Latakia Governorate, Tishreen University Journal for Scientific Research and Studies, Economic and Legal Sciences Series, 44(2):168 – 149 .
Rashwan , Abdul Rahman Muhammad Suleiman ; And Qasim , Zainab Abdel Hafeez Ahmed, (2022), The impact of cybersecurity risk management on supporting stability and financial inclusion in banks , the first international scientific conference entitled "The impact of cybersecurity on national security during the period 20-21 December 2022, Amman Arab University in association with the Public Security Directorate, 28:1.
Saleh, Nermin Muhammad (Determinants of the effectiveness of internal auditing for cybersecurity), 2022 Fifth Scientific Conference of the Accounting and Auditing Department (Challenges and Prospects of the Accounting and Auditing Profession in the Twenty-First Century) for the period from (10-11-2022).
Sandhu, S., & Arora, S. (2021). Customers' usage behavior of e-banking services: Interplay of electronic banking and traditional banking. International Journal of Finance & Economics, 27(2), 2169-2181. https://doi.org/10. 1002/ijfe.2266
Schwartz, M. J. (2013, March 21). South Korea Bank Hacks: 7 Key Facts. Dark Reading. Retrieved from https://www.darkreading.com
Security Scoreboard. (2016). Financial Industry Cybersecurity Report. New York: Security Scoreboard.

Shehata, Shehata Al-Sayed, (2022), Towards an effective role for the internal auditor in managing cybersecurity risks in companies listed on the Egyptian Stock Exchange, Scientific Journal of Financial and Administrative Studies and Research, 13(2): 37:26

Skinner, D. J., & Sloan, R. G. (2002). Earnings Surprises, Growth Expectations, and Stock Returns or Don't Let an Earnings Torpedo Sink Your Portfolio. Review of Accounting Studies, 7, 289–312.

Söylemez, S. A., & Ahmed, A. H. (2019). The role of new economic indicators on banking sector performance in Ghana: Trend and empirical research, analysis of banks' clients and experts' perception. Journal of Finance and Economics, 7(1), 23-35.

Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. Decision Support Systems (75), 49–62.

Sulaiman, N., Hamdan, A., & Al Sartawi, A. (2022). The Influence of Cybersecurity on the Firms' Financial Performance. In Future of Organizations and Work After the Fourth Industrial Revolution: The Role of Artificial Intelligence, Big Data, Automation, and Robotics (pp. 443-461). Cham: Springer International Publishing.

Trautman, L. J., & Altenbaumer-Price, K. (2010). The board's responsibility for information technology governance. J. Marshall J. Computer & Info. L, 28, 313.

Toivanen, H. (2015). Case study of why information security investment fail?. Master's Thesis, 76. Jyväskylä, Finland: University of Jyväskylä

Vagle, J. (2020). Cybersecurity and Moral Hazard. Stanford Technology Law Review, 23.

Yaqoub, Ibtihaj, Wahhab, Asaad, and Al-Fartusi, Ali (2022), A proposed indicator for accounting disclosure of cyber risks in the Iraqi Stock Exchange in accordance with international requirements: An experimental study, Journal of Financial, Accounting and Administrative Studies, 9 (1): 1403- 1430. Retrieved from https://www.asjp.cerist.dz/en/article/192579